International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-7, Issue No.-4, July, 2019

Studies on Secure Energy Efficient Routing Algorithm in WSNs

Rajiv Ranjan Tewari
Department of Electronics And Communication
J.K. Institute Of Applied Physics And Technology
University of Allahabad, Allahabad, India
E-mail: tewari.rr@redi mail.com

Snehi Saraswati
Department of Electronics And Communication
J.K. Institute Of Applied Physics And Technology
University of Allahabad, Allahabad, India
E-mail: snehisaraswati@gmail.com

Abstract: The evaluation of minimum spanning tree is helpful in the transmission of route data to a sink node during huge scale sensor network. In this route,a node may compromised and compromised node may be included and false data can be injected. It is also possible that the compromised node can change the existing data. In these circumstances, a Compromised node Locator protocol (COOL) is to be used to provide a security in Wireless sensor networks. COOL is su cient to remove compromised node from the WSNs. In case of detection of compromised node, this protocol can help to prevent more damages from unnatural/ unbehaved node.This constructs an energy saving and reliable WSNs. There is a need of technique or algorithm in which a path should be formed having minimum spanning tree by which the COOL protocol (security) in WSNs is to be maintained. It is challenging task to combine COOL protocol and MST (minimum spanning tree) and creates an energy conserving and secure WSNs. During these process sensor nodes communicates through our sink nodes. All other nodes send the data through routing by the sink node. The hash values are to be used to check the consistency of nodes.

Keywords:

I. INTRODUCTION

It is observed that WSNs have several applications in health, military and social sectors. The WSNs have following limitations:

1. Small tiny devices (sensor networks)
2. Limited storage capacity
3. Low battery power
4. Low computational capacity

The wireless sensor networks are deployed in an environment. The sensor nodes are left without taking into account to sense the data and its collection after deployment of the sensor nodes in the environment. The nodes send the data to the sink in such a manner that there is no loss of information. After sending the data to the sink, the sink node transfers it to the base station. The required data are collected in base station. It may be manipulated as per need and the decisions are taken at base station.

Figure 1 illustrates the basic functionality of a WSNs. If the data has been send to the sink node then there is a loss of energy. This happens because the transmitted data goes to multiple nodes.

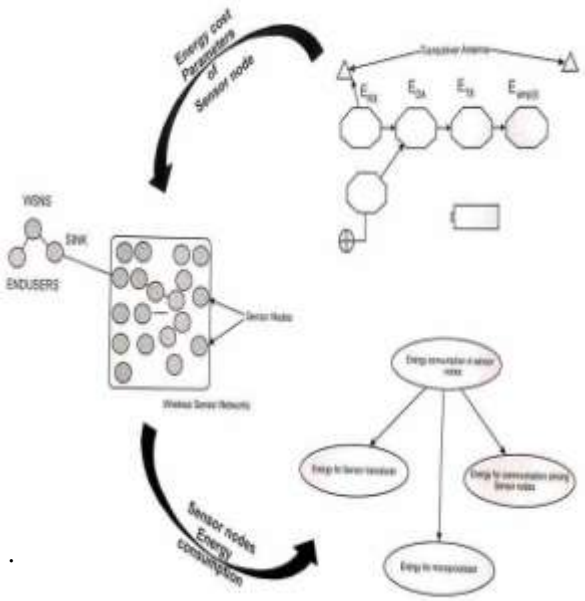

Figure 1: Basic functionality of WSNs

The multiple nodes are in position to transmit redundant data. Under these circumstances an e cient routing protocol is essential for following purposes:

(i) To perform efficient transfer of data.

(ii) To save battery power of sensor nodes.

Routing protocols are generally consisted of two main parts:

1. Tree based routing protocols 2. Cluster based routing protocols

By these protocols, data is sent to the sink node.

Topology construction is a challenging task in WSNs. In e cient topological construction, several parameters are to be taken in account. In general, efficient techniques should have following properties:

(i) ability to run in distributed environment.
(ii) low environment complexity.
(iii) enable to run without any additional hardware efforts.
(iv) produce a connected network by covering minimum number of sensor nodes.

The proposed technique can be able to run in huge WSNs. It is comfortable to run in devices with less computational work so less battery power is consumed. During this process, low cost and less energy consumption are to be maintained without the help of global positioning system (GPS). It is better if minimum number of nodes is required to connect WSNs.

Secure energy effcient routing techniques have been studied by several researchers like Porta et.al[1], Kang et.al[2], Zhang et.al[3], Tan et.al[4], Srinivas et.al[5]. In this paper, wiener index spanning tree is to be used for the purpose of transferring data from source to sink node. The concept of a watchdog node is introduced for the sake of security in attacks on sensor networks. The data is sent from source to the sink through the path generated by wiener index spanning tree. The best possible path is selected from the graphs generated by it. During the generation of all possible paths, certainly the cost is increased. It is remarkable to note that the consumption of energy is reduced in this process.

The watchdog node helps to monitor each node by other nodes neighbour to each other.It tries to nd out the availability of any misbehaving node. There are some limitations of watchdog node. It specifies the presence of misbehaving node only and helpless to locate it. Under these circumstances, the aim of this paper is to develop the algorithm having following properties:

(i) To make secure and energy efficient routing for WSNs
(ii) To save the power of nodes.
(iii) To solve the issue of watchdog node
(iv) To defne/ introduce a COOL protocol to identify and to remove the misbehaved node from WSNs.
(v) To use spanning tree topology to save the energy of node
(vi) To select the path for node which transmits data to the sink.
(vii) To apply COOL protocol to secure the information on the path of COOL protocol.

II. ENERGY CONSTRAINTS IN WSNS

Energy is one of the major constraints in WSNs. The life time of a sensor depends on the efficiency of source of energy. Four major components of sensor node architecture are given below :

1. Receiver 2. Data processor 3. Transmitter
4. Transmit amplifier

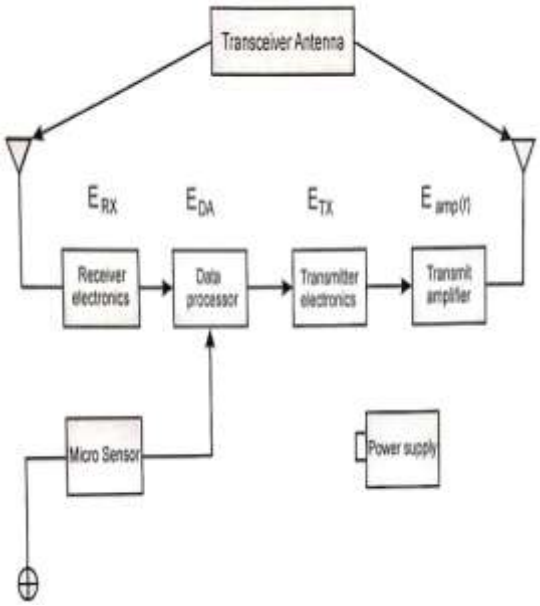

Figure 2: Major Components and associated energy cost parameter of a sensor node

The associated parameter for 1-4 are E_{RX} , E_{DA}, $E_{T\ X}$ and $E_{amp}(r)$ respectively. These facts are illustrated in figure 2. The consumption of energy in sensor nodes are classified into following parts:

(i) Energy for Sensor transducer
(ii) Energy for microprocessor computation and
(iii) Energy for communication among Sensor nodes

The cost of communication is more than computation cost and the energy is involved in many operations of WSNs. Due to this reason, the reduction of energy consumption is the current research issues.

The power consumption by sensor nodes is influenced by mainly following factors:

1. decryption 2. encryption 3. signing data 4. verifying signatures etc.

The security enforce overhead to power consumption. The security parameters are required in storing the energy. Consequently, the energy needs to transmit the security parameters. The complex security mechanisms require huge energy for the expansion of massages.

III. ROUTING CHALLENGES IN WSNS

The challenges in WSNs are mentioned as following:

(i) Limited bandwidth
(ii) limited power supply
(iii) deployment in the dense environment
(iv) through sink node, sensors sense/send the required data, then collect it and send to the base station. This is a time - taking process.

(v) the sensed data transfers to neighbour node and neighbour node sends the data back to the parent node. The multiple copies of the same data may be received by sink node. During this process, a big loss of power is observed. Thus, there is a need of a suitable routing protocol.
Major challenges in routing and design are as following:

A. *Node deployment*

Node deployment affects the working of the routing protocol. Two types of its deployments are as following:
1. deterministic deployment and 2. randomized deployment.
In deterministic deployment, the sensor nodes are connected and routing of connected data is generally through previously determined path.
In second case, randomly, nodes are scattered and infrastructure may be created in an ad-hoc manner.

B. *Energy consumption maintaining accurancy*

In WSNs there is a major role of supply of energy to sensor nodes for computation and transmission of data. The source of energy is an important component which affects the lifetime of sensor nodes. The failure of power causes the following disturbances in WSNs:
(i) malfunctioning of nodes (ii) topological changes
(iii) routing of packets and organizing of network.

C. *Data reporting modal*

This modal is concerned with applications and the time of data reporting. In this modal, following parameters are considerable:
1. time - driven 2. event – driven 3. query - driven and 4. hybrid

D. *Node/ Link Heterogeneity*

It several WSNs, the equal capacity of communication, power and computation is required for homogeneity. The technical issues are observed due to heterogeneous network.

E. *Fault Tolerance*

Some sensor nodes may be failed due to following reasons:
Lack of power 2. physical damage and
3. environmental interference
The performance of the network should not be affected due to failure of sensor nodes.

F. *Scalability*

Scalability of sensor node should be sufficiently enough so that using routing protocol be capable to work in the sensing reason.

G. *Network Dynamics*

There are two categories of sensor nodes :
stationary sensor node 2. Moving sensor node
Mostly sensor nodes are stationary but sometime movable sensor nodes are required. Hence the routing in moving node is presently more challenging nodes among these two.

H. *Transmission Media*

It is found that WSNs are connected to the wireless medium in the manner of multi - hop. The high error rates and fading are problems associated with wireless channels. These problems affect the operations of the sensor nodes.

I. *Coverage area*

At the time of designing of WSNs, the researchers consider the coverage area. The range and accuracy are the important parameters in a coverage area of a node.

J. *Connectivity*

The connectivity of WSNs depends on the distribution of node. Highly connected nodes are expected by the researchers to fulfill the requirements of the modern society.

K. *Data aggregation*

There is a need of data aggregation in achieving energy efficiency and data transfer optimization.

IV. ENERGY EFFICIENT HIERARCHICAL ROUTING ALGORITHM

One of the main research field in WSNs is HWSNs. It behave the most energy efficient among the remaining protocols for WSNs. The classification of routing protocols is given in the following figure 3. The researchers have proposed for the routing the correct information to the base station (B.S.) keeping in mind the prolonging the life of concerned sensor nodes. Under the circumstances, there are limited advantages and disadvantages of each protocol.

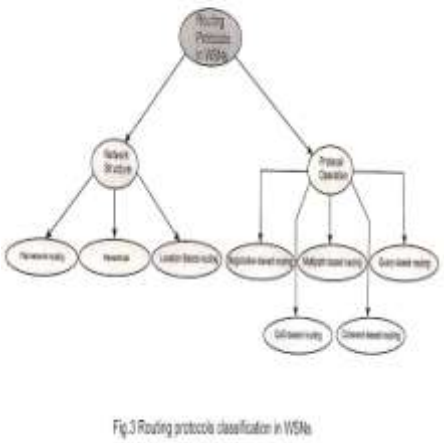

Figure 3: Routing protocols classification in WSNs

L. *Routing Protocols*

Generally, routing protocols are divided as per their functioning:

1) Negotiation based routing

High level data descriptors are used for negotiation to reduce redundancy in data transmission. If the real data transmission takes place then it reduces the redundant information. consequently the redundant data is removed and necessary data is transferred to next hop based in the series of the negotiation messages. SPAN is one of examples of this routing.

2) Multipath based routing

In the unreliable environment this routing is applied to deliver the data for increasing the reliability of WSNs.The traffic is increased due to many paths from the source to destination. In spite of this, the reliability is improved. Hence, there is a tradeoff between reliability and traffic. The tradeoff is considered as a function which depends on following parameters:
Degree of multipath 2. failing probability of available paths
The original packet has been broken into subpackets. The subpackets are sent over multiple path. The original massages are reconstructed at the destination even in case of loss of some subpackets.

3) Query Based Routing

A query for the data is to be generated by sink node or destination node. This is to be sensed by the sensor nodes. A node or more than one node sends the data to fulfill the requirements of the query. Then it is to be propagated by the destination node.

4) Quality of service based routing

QOS based routing helps to provide the balance between energy consumption and data quality. QOS metrices give the information of bandwidth, delay, energy and other parameters. SAR (Sequential Assignment Routing) is an improvement of QOS based routing. The routing decision is based on the following factors:
energy resources 2. QOS on each path 3. priority level of each path
In this routing, multipath and localized path restoration path schemes are used to neutralize the single path failure.

5) Coherent Based Routing

There are two categories of data processing:
Coherent data processing and 2. Non-coherent data processing.

In second category, sensor nodes send raw data to the other nodes for processing. In case of first category, the data is send to the aggregators after less processing like duplicate suppression and time stamping. Cohrent based routing is considered to accomplish energy efficient routing.

M. *LEACH (Low Energy Adaptive Clustering Hierarchy)*

Using homogeneous stationary notes, LEACH considered to improve the energy - efficient hierarchical routing protocol. In LEACH, sensor nodes select their parameters depending on strongest signal received from a CH. After fixed interval, new nodes are considered as CH. During this process, LEACH may help in reducing the energy consumption. It utilizes the rotation of CHs to distribute the load of energy in WSNs. The ordinary nodes are turned off when there is no their utility.

N. *PEGASIS(Power-Efficient Gathering in Sensor Information Systems)*

PEGASIS is an improvement of LEACH protocol. A suitable chain has been formed from sensor nodes. The data are received or transmitted by sensor nodes from their neighbour. The advantages of PEGASIS are mentioned as following:
(i) It avoids cluster formation.
(ii) Only one node is used in a chain for the transmission to the base - station. and
(iii) Thus, PEGASIS increases the lifetime of the network.

O. *HEED (Hybrid Energy-Efficient Distributed Clustering)*

HEED is an extension of LEACH. CHs are to be selected randomly in HEED clustering. It improves the network lifetime over LEACH clustering.

P. *EEHCA (Energy-Efficient Homogeneous Clustering Algorithm for WSNs)*

During this algorithm, on the basis of residual energy of existing CH, a new CH is selected. It is nearest to hop distance of the node and holdback value. Thus, the network lifetime may be extended due to uniform distribution of members of the cluster.

V. SECURITY REQUIREMENTS IN WSNS

The components of security requirements in WSNs is mentioned in the following figure 4

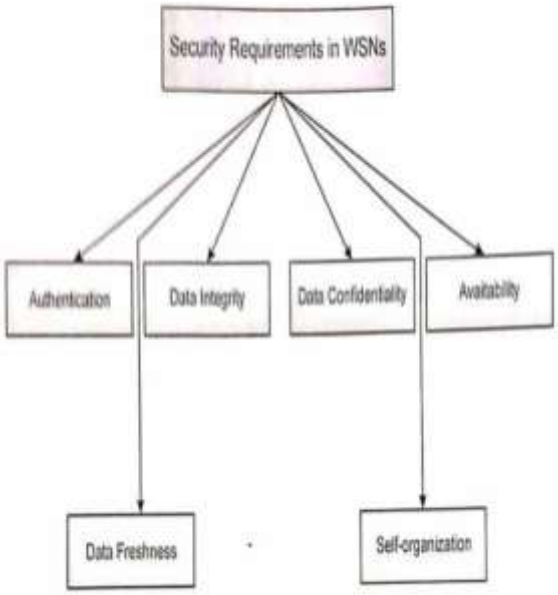

Figure 4: Security requirements components in WSNs

Q. Authentication

Authentication identifies and controls the participants in WSNs with security. The consumer wants to see the authentication as the cornerstone of a node. If the messages are communicated with the correct nodes then there is a possibility of ensuring confidentiality and integrity of exchanged messages. There is a need of mechanism to verify the receiving of packets from the actual sender node. MAC (Message Authentication Code) should be used to ensure the integrity and authentication of the origin of the message. HMAC is an example of MAC.

R. Data Integrity

Data integrity ensures that messages travels from sender to the recipient without any change. Cryptographic hash functions are requiring a fingerprint of each digital message. The examples of generally used hash functions are
1. Secure Hash Algorithm - 1 (SHA - 1) and 2. MD 5 function

S. Data Confidentiality

Symmetric as well as asymmetric cryptography keys are used to ensure confidentiality and secrecy of exchanged messages.

T. Availability

Availability always ensures the services of WSN ignore the internal and external attack. The successful delivery of message to its recipient is ensured by using a central access control system.

U. Data Freshness

Up-to-date data is an essential part of Data Freshness. The old messages should not be replayed. During message communication, shared keys are used by sensor nodes. A replay attack is observed when old key is used so new key should be refreshed. It is propagated to all concerned nodes. The freshness of the packet may be checked by an additional time-specific counter.

V. Self-Organization

Each node of a WSN should be self-organized in nature. The security is involved in self-organized nodes. The mechanism for pre- installment of shared key is needed due to dynamic nature of a WSN.

VI. ROUTING ATTACKS IN WSNS

Many security attacks in WSN are mentioned below:
1.Sybil 2. sinkhole 3. hello flood 4. wormhole 5. selective packet forwarding 6. spoofed, Altered and replayed routing information.

W. Sybil Attack

In sybil attack, the attacker damages the routing mechanism. Validation techniques prevent this attack.

X. Sinkhole Attack

The sinkhole attack causes another attacks like blackhole, selective forwarding, etc.

Y. Hello Flood Attack

In this type of attack, attacker broadcasts hello message to every node in WSN. Other nodes receive this message. Thus attack is possible. The blocking techniques may help in prevention of Hello flood attacks.

Z. Wormhole Attack

It is very difficult to detect wormhole attack using out-of-bound channel to route packets.

AA. Selective Forwarding

Following two factors play important role in selective forwarding :
(i) The location of attacker is to be taken in account because several nodes are affected if the location of attacker is very close to base.
(ii) The number of unused messages is second factor in selective forwarding.If the number of dropped messages

increases then more energy is to be attacked. Thus an adversary may selectively forward suitable messages and drops others selectively to compromise a node.
Give table 1 explains some important attacks on WSNs and their solutions to defeat them

Layer	Attacks	Solutions
Network	Spoofed routing information send selective forwarding	Authentication, Monitoring egress filtering
	Hello Flood	Packet leashes using geographic and temporal info
	Warmhole	Probing
	Sinkhole	Checking of redundancy
	Sybil	Monitoring, Redundancy

Table 1: Some important attacks on WSNs and their solutions

VII. IDEA OF WATCHDOG NODE

Some nodes are left unattended after deploying the WSNs in the environment. The unattended nodes make the possibilities of security attacks to send the false data report to sink node and base station. The watchdog node identifies this correct and false informations. It helps to send the correct data to the sink node. Hence, each node is monitored to avoid the false data report.
The watchdog node is unable to identify the misbehaving node. There is a need of protocol to identify the misbehaving node in WSNs. The figure 5 presents the mechanism of watchdog node. This mechanism depends on following conditions
z

Figure 5: Watchdog Node Mechanism

(i) Ambiguous Collision : If node A is transferring data to node B then it overhears that B is forwarding data to next hop but when B sends data to next hop then A will not overhear.
(ii) Receiver Collision : If node B sends data to node C and the data is dropped by C then there is a chance of overhearing and collision.
(iii) Limited Transmitted Power : There is a consumption of energy when B is forwarding the data to node C.
(iv) False Misbehavior: In case of sending the data to node B by node A, node S is overhearing for the purpose of monitoring. If node A sends data to B and B is dropping the packet then its work is like misbehaving node for the node S.

VIII. LOW LATENCY WIENER INDEX SPANNING TREE

WSNs have following limited capacities:
1. Small size
2. Low power capacity
3. Low cost
4. Multifunctional behavior
Thus, MWST (minimum wiener index spanning tree) should be used to flow the data through this path between nodes. The advantages of Wiener Indexed Tree are as following :
(i) The consumption of energy is minimum during transmission of data to nodes. In this case, the transmission distance of data is less as compared to other tree topologies.
(ii) The Wiener Index spanning obtains the best possible spanning tree.
(iii) Branch Bound and Simulated Annealing are two main protocol classifications of Wiener Indexed tree.

Simulated Annealing algorithm is used for large scale sensor networks. The Branch and Bound algorithm is found for small scale sensor networks.

BB. Branch and Bound Algorithm

It is used to solve optimization problems. The optimal solutions are obtained by this algorithm. The branch and bound algorithm is helpful to increase the functionality of backtracking. A searching technique for possible feasible solutions is a backtracking. It removes the search results in a specific region of solution space. The processes of this algorithm are as following :
(i) To minimize the search space by elimination of unnecessary sub-tree of solution space.
(ii) To update the upper bound and then compare it with bounding function value and
(iii) To improve the solution space tree of nodes in each step of this process.
This algorithm is not suitable for large scale WSNs. The search space is reduced during this process. This is a demerit of branch and bound algorithm. Hence, a new algorithm may be proposed for the large scale network. Simulated Annealing algorithm is one of them.

Algorithm 1 Branch Bound Algorithm
Input: No. of Node = M, Priority Queue, Graph =G, Degree
Output: Appropriate solution for Wiener Index Tree
1: **deftne struct** *node{*
2: **int** *L; // L = level of space tree*
3: **int** *P*[*M*]; *solution of vector space*
4: *LB = lower bound*
5:}
6: *node*

7: **Start**
8: *No. of node = z*
9: *ρ(span tree)→ upper bound // min spanning tree of Graph will be used to compute upper bound*
10: *insert(Priority Queue, → z)*
11: **while** Priority Queue is not empty **do**
12: *Delete Priority Queue→z*
13: **if** *z.LB < upperbound* **then**
14: *z.L + 1→q.L*
15: **for** *i←*1 to *M* + 1 **do** *// including all parent node*
16: *i→q.P[q.L]*
17: **if** *Solution is feasible* **then**
18: **if** *q.L = M* **then**
19: *ρ(q)→R* ;

20: **if** *R > upperbound* **then**
21: *R → upperbound// upper bound is updated* ;
22: q.P → minimum wiener index tree // appropriate solution is update
23: **else**
24: *Bounding(q)→q.LB*;// for node q value of
25: bounding function is obtained
26: **if** upper bound > q.LB **then**
27: insert (Priority Queue, q)
28: **End**

CC. *Simulated Annealing Algorithm*

This algorithm is used to find out solutions of complicated optimization problems. Suppose G is a given sensor network. The solution t_α is generated by this algorithm and the spanning tree is obtained. The detailed algorithm of simulated annealing is developed as following:

Algorithm 2 Simulated Annealing Algorithm
Input: Graph G
Output: Minimum Wiener Index Spanning Tree MWST
1: *Randomly generate an initial feasible solution* $t_\delta \rightarrow t$,
2: *Spanning tree from graph G*
3: *Compute Wiener index of initial solution* t_δ
4: *Determine an initial temporal* $TM_t \rightarrow TM$,
5: *and a final temperature* TM_t
6: *Determine temporal reduction rate* λ
7: **while** $TM > TM_t$ **do**
8: begin randomly select a neighbor solution t_γ *s M(t)*
9: **if** $\rho(t_\gamma) \leq \rho(t)$ **then**
10: $t_\gamma \rightarrow t$
11: **else**
12: uniformaly generate a random number R in the range (0,1);
13: **if** $R < e^{-\frac{\rho(t_\gamma)-\rho(t)}{TM}}$ **then**
14: $t_\gamma \rightarrow t$;
15: $TM \rightarrow \lambda \times TM$

DD. *Consumption of energy in Wiener Index Spanning Tree*

A round packet transmission is observed in Wiener Index Spanning Tree. A WSN collects the packet of equal length from each other node and after this, it transmits this packet to another nodes. Thus, the simulation environment is characterized. Any node in WSNs could be the nearest node to the moving base nodes. It would be the quick transmitter of packets to the sink. The concerned node behaves like a source code which collects signals and these signals are transmitted to target sink. The average hop count and energy consumption are main components of Wiener Index Spanning Tree. These components are required to evaluate and to compare the objective for the performance of routing trees. Figure 6 shows the energy consumption in Wiener Index Tree.

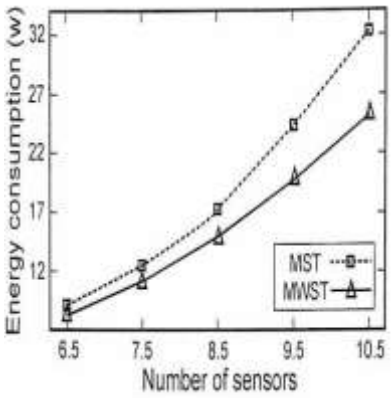

Figure 6: Energy Consumption

EE. *COOL Protocol*

The compromised node Locator protocol is written as COOL protocol. The main parameters in WSNS are as follows:
(i) The source of energy (ii) network lifetime and
(iii) security in sending information to the sink node.
Thus, COOL protocol helps to secure energy efficient routing through spanning tree path. During this protocol, following procedure is followed:
A path from source to sink node is stretched.
The hash for each node on that path is calculated.
The value of hash is obtained considering the transmitted data.
(iv) The Concerned data is sensed by the node in the environment of sense.
(v) COOL protocol is enabled to find compromised node is WSNs.

IX. PROPOSED RESEARCH WORK

In proposed algorithm, security and securing the information from compromised node are main issues which are to be achieved. Firstly, sensing nodes in sensing enviorments are to be deployed. The positions of nodes are located on X and Y co-ordinates axes. Applying MST (minimum spanning tree algorithm), the path of data flow to the sink is considered. After selection of suitable path, the information is sent on this path securely. By the concept of COOL protocol,

the security of the selected path can be checked. During this process, each node is assigned its own hash value. This hash value is sensed by the node from the environment. Following steps are followed during this algorithm:

Step 1: Deploy the sensor nodes in the suitable environment and the position of the sensor nodes are selected as following:
The range of X co-ordinates is between 0 to 250. The range of Y co-ordinates is between 0 to 250.
During this process, each node has its position. Considering the position of node, the next phase of algorithm is proceeded / performed. There may be some agent during deploying the nodes. These agents help the sink node during the operations they are used as per need of the user.
Step 2 : Minimum spanning tree (MST) algorithm is used to get the suitable path. The informations are sent from source to sink node through this path. The minimum spanning tree is obtained by PRIM's algorithm.
T=φ; A=1;
Define the starting vertex in the path while ($a \ f= b$)
{ Let (a,b) be the smallest edge weight such that

$a \in A, b \in B - A; T = T \cup \{(a,b)\};$

$A = A \cup b$

}
Step 3: Try to find hash value and hash number of the nodes: Hash number is obtained by the value sensed by nodes. Calculated hash number is transferred to the next node. Hash value is generally termed as "For examining the node consistency, hash number to be sent to the the next node in the path".
The addition of the hash value of previous node and current node hash number is the hash value. The node consistency is maintained by this process.

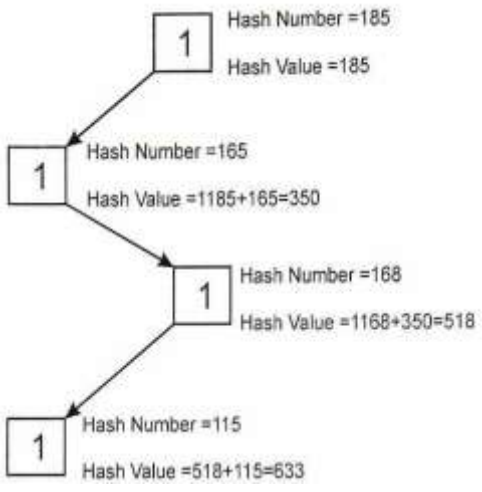

Figure 7: Generation of Hash number and Hash value

Step 4: Examine the condition for the integrity of hash between the nodes.
If (hash values of sender and receiver are same)
Then go to the next node and repeat the same procedure. Else
Backtrack to previous node and then verify the entry for hash value.
Step 5: (To find the misbehaved node in the network).
If (the consistency of all nodes is satisfied) Then
Send the information to the sink node. Else
Go to that node where consistency is not satisfied.
Step 6: Remove the misbehaved node from the network and examine the nearest node to the compromised node.
If (nearest node is observed in case of its presence)
Then Make a path to nearest node. Remove the previous node from the WSN. Examine the consistency for newly added node.
Else
Find the nearest node based on the location of WSN and then add that node to the network.

X. SIMULATION OF RESULTS

In the proposed work, the sensor nodes are installed at required location in the enviorment. Using PRIM's algorithm based on the position of sensor nodes, the minimum spanning tree is evaluated. In this manner, the unique path from source to destination is obtained The hash number is observed by all sensor nodes in the spanning tree and it is kept in a local database. The inconsistency between two nodes in the path can be removed by applying backtracking to find out its location. After recognition the location, the inconsistent hash value is observed. If the hash value of the sender node is same the hash value of receiver node then this node is a compromised node. A node is selected nearer to the sender node in the path. It should behave like a normal node. This node is not faulty node. The data is sent to the near one node and this newly selected node continues this process in the same path. In this process, the effect of the family node is neutralized. Before sendind data to newly selected node, its consistency should be checked. Suppose this is also behaved as faulty node then again the nearer node is selected and repeating the previous procedure, it should be removed. The data is transferred from the source to the destination successfully in WSNs.
Figure 8 shows throughput comparison graph between the proposed algorithm and previously existing algorithm which is wiener index. The proposed algorithm generates the high throughput as well as secure path through which data is sent to the sink node. The time is presented on the x-axis and number of packets sent in each unit is located on the y-axis. The shows the comparison based on packet drop in proposed algorithm and the existing algorithm.

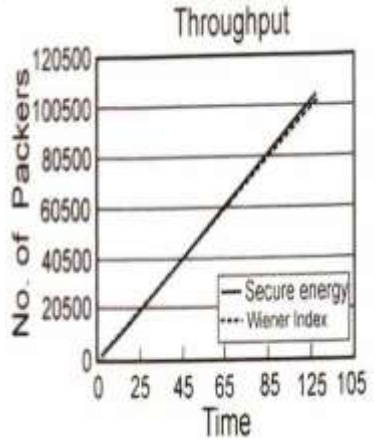

Figure 8: Throughput comparison graph

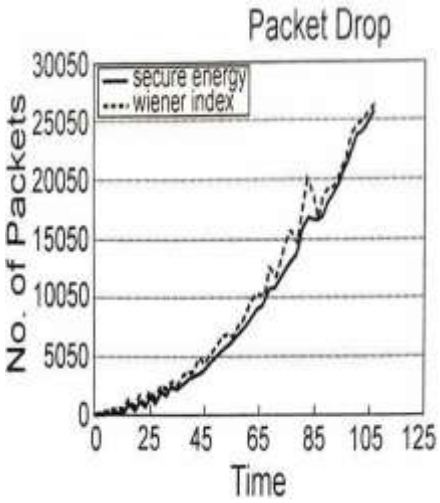

Figure 9: Packet drop comparison

The demerits of previous existing algorithm are mentioned as following:
(i) There are tremendous packet loss.
(ii) It is applicable for several possibilities of spanning tree to send the data to the sink.
(iii) The watchdog node monitors the neighbour node by its packet log.
(iv) There are loss of data in maintaining the log to packets.
Figure 10 explains the energy consumption in sensor network nodes in unit time.

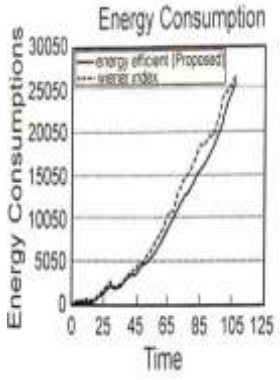

Figure 10: Energy Consumption in Sensor Network

XI. CONCLUSIONS

The conclusions of this research papers are as follows:
(i) In proposed algorithm, the data is sent from the source to the destination after the verification of its safety.
(ii) The steps of procedure are completed on the basis of hash value.
(iii) The hash value is verified by the packet.
The security of the path is checked.
(iv) The packet loss is minimum during proposed algorithm in comparison of previous algorithm.
(v) The path is created from the source to sink node and watchdog node is used to monitor all nodes of WSNs by their neighbor nodes.
(vi) A COOL protocol is applied to prevail over the issue of watchdog node.
(vii) This protocol helps in finding and removing the misbehaving node.

REFERENCES

[1] Cao G. Porta,TL Wang G., Zhang W,"On supporting distributed collaboration in sensor networks", IEEE MILCOM, 2003, 3, 14, 15.

[2] Seung-Ho Kang, Seung-Wan Han, in-Seon Jeong, "Low latency and energy efficient routing tree for wireless sensor networks with multiple mobile sinks", Journal of Network and Computer Applications, 2013, 3, 17, 18.

[3] Youtao Zhang, Jun Yang, Lingling Jin and Weijia Li, "Locating Compromised Sensor Nodes through incremental Hashing Authentication", Distributed Computing in Sensor Systems, Lecture Notes in Computer Science, Vol.4026, pp 321-337, Springer link.

[4] Huseyin Ozgun Tan, Ibrahim Y. Sankarasubramaniam, E. Cayrci I.F., Akyildiz and W. Su, "Wireless Sensor Networks: A Survey", Elsevier, 2001,1,2.

[5] K. Srinivas, A. Venugopal Reddy, A. Nagaraja, "Wireless Networks Coding: An Innovative Technologgy", proceeding of 2013 International Conference on Green Computing Communication and Conservation of Energy(ICGCE- 2013), organized by RMD Engineering College, Chennai, India, Dec 2013.